

SEMINARIO PER DEONTOLOGIA ED ETICA PROFESSIONALE - Edizione anno 2025

Perugia 30/05/2025

Protezione dei Dati Personali

Profilo personale

- Dal 2004 socio ed amministratore dell'azienda di consulenza LUSIOS SRL.
- Sistemista esperto ed auditor ISO 9001, ISO 14001, ISO 45001, legge 231,
- Amministratore di sistema e coordinatore dei sistemi informatici
- Esperto ed auditor di terza parte di sistemi di gestione ISO 27001, ISO 27017 ed ISO 27018,
- Analista di Sistema per sviluppo software e valutazione della sicurezza di sistemi informatici.
- DPO certificato secondo UNI 11697 da Accredia.
- Consulente e Formatore in materia di Privacy e Whistleblowing, Direttiva NIS2

Definizioni

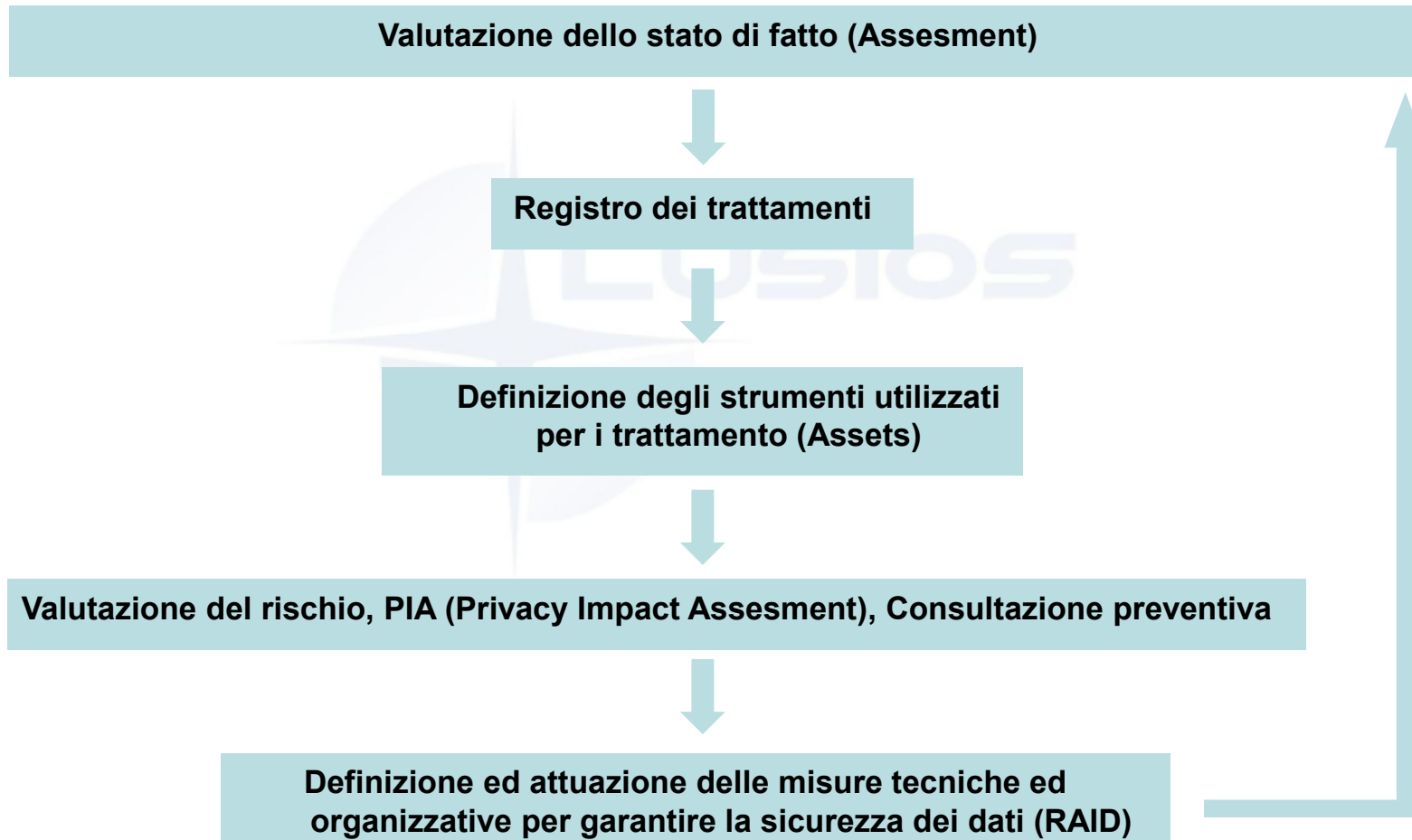
- **Titolare del trattamento:** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
- **Interessato:** Soggetto del quale vengono trattati i dati.
- **DPO/RDP Responsabile della Protezione dei Dati o Data Protection Officer:** la persona fisica o giuridica nominata dal responsabile o dal titolare del trattamento che ha compiti di: Sorveglianza, Consulenza e di interfaccia con l'autorità di controllo.

Categorie di dati

- **Dati Personali:** qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)
- **Dati Particolari** (prima sensibili): dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.
- **Dati Giudiziari:** dati relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

NOVITA' DEL GDPR

APPROCCIO ALLA GESTIONE DEL PROCESSO PRIVACY



Registro dei trattamenti

Uno strumento per mappare i trattamenti effettuati: obbligatorio per aziende con più di 250 dipendenti o in caso si trattino dati particolari.

In realtà strumento fondamentale di mappatura dei dati dell'organizzazione.

Responsabile Ex Art. 28

Responsabile: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

Obbligo di nomina (atto giuridicamente vincolante)

Data Breach

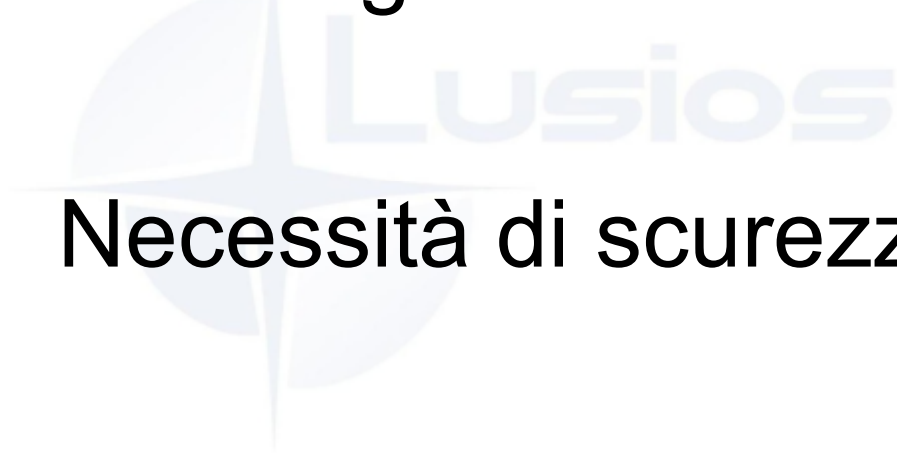
OBBLIGHI DEL TITOLARE IN CASO DI DATA BREACH!:

- 1) Notifica al garante entro 72 ore dalla notizia se il data Breach rappresenta un pericolo per i diritti e le libertà dell'interessato
- 2) Informazione agli interessati se il data Breach rappresenta un elevato pericolo per i diritti e le libertà dell'interessato

COSA E' NECESSARIO FARE?

Obblighi normativi

Necessità di sicurezza



Informative e consensi

Ogni qual volta acquisiamo dati dall'interessato dobbiamo spiegare come utilizzeremo i suoi dati.

A margine dell'informativa può essere richiesto (se previsto dalla normativa) il consenso al trattamento dei dati.

Nomina degli autorizzati al trattamento

Il personale che gestisce dati sotto il controllo del titolare del trattamento deve essere formalmente incaricato (e ove previsto anche con istruzioni scritte) in relazione ai dati che tratta.

Formazione

Il Titolare del trattamento deve formare il personale che opera sotto il suo controllo autorizzato ai trattamenti sulla conoscenza del GDPR (Regolamento europeo 679/2016)

Come muoversi adottando misure di sicurezza adeguate

(misure di igiene informatica di base)

BACKUP

- **Backup multipli**
- **Backup geolocalizzati**
- **Storicizzazione dei Backup**
- **Verifica di Restore**
- **Backup Immutabili**
- **Soluzioni NAS**
- **Soluzioni Cloud**

Come scambiare dati in sicurezza

- E-mail è sicura?
- La PEC (Posta Elettronica Certificata) è sicura?
- Dispositivi (Chiavette USB o HD removibili) sono sicuri?
- Sistemi di scambio dati via E-mail (WeTransfer) è sicuro?
- Il Cloud è sicuro?



II FIREWALL

- Cos'è?
- A cosa serve?
- Sistemi IPS
- Sistemi IDS
- Sistemi di conservazione
E management dei log



Gestione delle password

- Concetto di robustezza di una password
- Ricerca in forza bruta cos'è e come difendersi
- Perché cambiare le password frequentemente
- Usi sempre la stessa Password o sono simili?



Accesso ai dispositivi con metodi biometrici

- Impronta digitale
- Immagine del volto
- Impronta vocale
- Password manager



Soluzioni avanzate di sicurezza

- Virtualizzazione dei server
- Soluzioni avanzate: Iperconvergenza
- Sistemi Controllo dei Log (SIEM)
- Sistemi SOC (Security Operation Center)
- Sistemi di Threat Intelligence
- Vulnerability Assessment
- Penetration Test
- WAF (Web Application Firewall)
- XDR (Extended Detection and Response)



GRAZIE PER L'ATTENZIONE

Ing. MICHELE MERCANTI

Via della Martinicca, 36 Perugia

Tel.: (+39) 075 609699 – (+39) 340 1298071

E-mail: michele.mercanti@lusios.it

DPO certificato UNI 11697 Intertek ACCREDIA